Criptografía y Sistemas Móviles

Castro Lechtaler, Antonio[1, 2]; Cipriano, Marcelo[1;3]; García, Edith[1],
Liporace, Julio[1]; Maiorano, Ariel[1]; Malvacio, Eduardo[1]; Tapia, Néstor[1];

[1]Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática.
Escuela Superior Técnica, Facultad del Ejército. Universidad de la Defensa Nacional UNDEF.
[2] CISTIC/FCE - Universidad de Buenos Aires.
[3] Departamento de Ciencia y Tecnología, Universidad Nacional de Quilmes UNQ.

acastro@est.iue.edu.ar , marcelocipriano@est.iue.edu.ar,
{edithxgarcia; jcliporace; maiorano; edumalvacio; tapianestor87}@gmail.com

RESUMEN

Este proyecto persigue el estudio, diseño y desarrollo de un Algoritmo de Cifrado en Cadena o Stream Cipher, que pueda ser ejecutado sobre un sistema móvil (teléfono celular, tablet, radios que operan en bandas VHS, UHF o cualquier otro dispositivo de similares características) para así poder ofrecer confidencialidad a la información transmitida.

Tal algoritmo deberá ofrecer capacidades especiales, como trabajar en altas velocidades de cifrado/descifrado, robustez y resistencia a los ataques criptoanalíticos conocidos, tales como el Criptoanálisis Diferencial [1], Criptoanálisis Lineal [2], Cube Attack Cryptanalysis [3-4] y otros [5-6].

Para ello se seguirá la filosofía de diseño y construcción en la que atendiendo los ataques conocidos el algoritmo se diseña resistente a dichos ataques [7].

También se tendrá en cuenta que dicho algoritmo debe ejecutarse en forma eficiente en dispositivos reducidos en tamaño, potencia de cómputo, capacidad de memoria y consumo eléctrico, entre otras. Ya que muchos de los sistemas móviles priorizan la movilidad, liviandad de los equipos, reducidos consumos eléctricos para prolongar la carga de la batería y demás limitaciones que conspiran contra el normal desempeño de un algoritmo criptográfico.

Palabras Clave:

Criptografía. Criptoanálisis, Criptosistemas de Clave Privada, Stream Ciphers. Sistemas Móviles.

CONTEXTO

En el marco de la carrera de grado de Ingeniería en Informática y el posgrado en Criptografía y Seguridad Teleinformática que se dictan en la Facultad de Ingeniería del Ejército (FIE) "Gral. Div. Manuel N. Savio", Universidad de la Defensa Nacional (UNDEF) se llevan adelante tareas de I+D+i por parte del Grupo de Investigación en Criptología y Seguridad Informática (GICSI).

GICSI depende del Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática (CriptoLab) perteneciente al Laboratorio Informática (InforLab). Y está conformado por docentes investigadores, profesionales técnicos y alumnos de dicha área.

1. INTRODUCCIÓN

A la población en general parece no importarle (o al menos eso parece) la confidencialidad de sus comunicaciones. La información que nuestros dispositivos de redes y comunicaciones procesan y transmiten, están sometidos riesgos más allá de los ataques de hackers u otros. El riesgo que gobiernos y empresas puedan acceder fácilmente a la información. Esto quedó expuesto a nivel mundial en la masacre de San Bernardino de 2015[1]. Más allá del lamentable suceso, se originó una discu-

[1] Hecho luctuoso que se realizó durante un banquete del Departamento de Salud Pública realizado en un centro para personas con capacidades diferentes del condado de San Bernardino, California (Estados Unidos) el 2 de Diciembre de 2015. Allí 2 terroristas dispararon contra los comensales hiriendo al menos a 21 personas y asesinando a 14. Uno de ellos era empleado en ese lugar y compañero de muchas de las víctimas.

sión ética y legal entre la Oficina Federal de Investigación[2] y la empresa Apple pues la policía encontró un teléfono iPhone 5C, propiedad de uno de los terroristas. El FBI le exigía a la empresa que "abra" el móvil que se encontraba bloqueado y su contenido cifrado con AES-256[3]. En particular solicitaban que se les entregue una especie de "llave maestra" del cifrado, una "puerta trasera" del sistema operativo iOS del teléfono o en su defecto que la empresa Apple intente hackear su propio teléfono, para acceder a la información almacenada en él.

La empresa se negaba a hacerlo alegando que no podía atentar contra la confidencialidad de sus usuarios y que además eso iría contra los intereses comerciales de la misma ya que entonces sus clientes podrían dejar de usar sus teléfonos o dejar de comprarlos.

La controversia pronto escaló hasta la justicia estadounidense. Luego de un tiempo litigando en los tribunales, discutiendo en las redes sociales y los medios de comunicación, el gobierno desistió de la demanda: ya lo habían resuelto por su cuenta… es decir… pudo acceder a la información almacenada en el equipo.

Como usuarios tenemos pocas herramientas a nuestro favor que nos permitan proteger nuestra información. Desde la empresa que diseña, fabrica y comercializa los equipos (tanto computadoras, tablets, móviles y demás) hasta la infraestructura de Internet, nuestra información es procesada, almacenada y transmitida con escaso o nulo control sobre ella.

El Grupo de Investigación en Criptografía y Seguridad Teleinformática (GICSI) por medio de este proyecto intenta ofrecer un mecanismo de seguridad para preservar la confidencialidad de la información mediante el uso de un mecanismo de cifrado robusto y adaptado a sistemas móviles.

Muchos de estos sistemas tienen amplios recursos de hardware y software (algunos teléfonos móviles sorprenden por las altísimas prestaciones que ofrecen, gracias a la potencia de su hardware), otros en cambio, tienen reducidos recursos para lograr sus objetivos. Tal es el caso de sistemas que al priorizar la movilidad o portabilidad de los mismos, deben reducir su tamaño, peso, capacidad de almacenamiento, cómputo y consumo energético, por mencionar algunas de las restricciones.

Esa reducción no debiera influir en la disminución de la confidencialidad que tales equipos requieran. Existen mecanismos criptográficos que permiten ofrecer la robustez necesaria aún en contextos limitados.

CriptoLab desde el ámbito académico ha realizado algunas propuestas para vehículos aéreos no tripulados del Proyecto LIPAM del Ejército Argentino, los cascos de realidad aumentada del Proyecto[4] RAIOM del Centro de Investigaciones para la Defensa - CITEDEF[5]. También se pueden mencionar otros sistemas y vehículos militares, como el PANHARD francés que el Ejército y otras fuerzas poseen y que la FIE recibió como encargo, llevar adelante su modernización.

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO

Para llevar adelante el proyecto, se ha dividido en 4 etapas de investigación y desarrollo:

- Estudio y análisis de algoritmos que satisfacen los requerimientos y condiciones de entorno del proyecto.
- Personalización, diseño, desarrollo del algoritmo e inclusión de mejoras.
- Determinación de las propiedades criptológicas.
- Ejecución de los tests y demás pruebas.

[2] En inglés: Federal Bureau of Investigation. FBI.

[3] AES: en inglés Advanced Encryption Standard. Algoritmo criptográfico de 256 bits de clave privada, que se convirtió en un estándar del NIST en 2002. A la actualidad es considerado seguro y resistente a los ataques conocidos… ¿o ya no?

[4] RAIOM: Realidad Aumentada para la Identificación de Objetivos Militares.

[5] CITEDEF: El Instituto de Investigaciones Científicas y Técnicas para la Defensa; ex Instituto de Investigaciones Científicas y Técnicas de las Fuerzas Armadas (CITEFA)

3. RESULTADOS OBTENIDOS/ESPERADOS

La persigue el diseño de un mecanismo de cifrado tipo Stream Cipher que dote de confidencialidad a las comunicaciones de un Sistema Móvil. Que pueda además demostrar su fortaleza al resistir los ataques criptoanalíticos conocidos.

La realización de un desarrollo propio y nacional no sólo permitirá ofrecer una capa más de protección a la información respecto a la confidencialidad de la misma por medio de un algoritmo criptográfico, sino que además permitirá ahorrar recursos económicos. El costo de desarrollar un algoritmo puede apreciarse más beneficioso que la adquisición de uno extranjero, sobre todo por el alto costo de los mismos, valuados en moneda foránea.

4. FORMACIÓN DE RECURSOS HUMANOS

Los docentes investigadores del proyecto dictan las asignaturas Criptografía y Seguridad Teleinformática, Matemática Discreta y Paradigmas de Programación I, II. Desde esas cátedras se invita a los alumnos a participar. Es por ello que 3 de ellos han demostrado su interés y se han sumado en calidad de colaboradores. En particular, el alumno Leiras, Facundo ha presentado su postulación en 2018 para la beca "Estímulo a las Vocaciones Científicas" (EVC) otorgadas por el Consejo Interuniversitario Nacional (CIN) por encuadrarse en las condiciones requeridas[8]. La misma le ha sido otorgada, iniciando en breve sus actividades respectivas.

Se desea destacar que el incremento del Know-How que tendrá el grupo de investigadores a lo largo de la vida del proyecto será una importante y económica Formación de Recursos Humanos en beneficio de sus integrantes y de la institución en la cual desarrollan sus actividades científico-docentes.

Por último y atendiendo a la responsabilidad ética y social que compete a la actividad científica y tecnológica, el Grupo Integrante de este Proyecto de Investigación, ya sea durante su ejecución o por la aplicación de los resultados obtenidos, desea expresar su compromiso a no realizar cualquier actividad personal o colectiva que pudiera afectar los derechos humanos, o ser causa de un eventual daño al medio ambiente, a los animales y/o a las generaciones futuras.

5. BIBLIOGRAFÍA

[1] Wu H., Preneel B. *Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy*. In: Naor M. (eds.) Advances in Cryptology. EUROCRYPT 2007. Lecture Notes in Computer Science, vol. 4515. Springer Berlin, Heidelberg. 2007.

[2] Muller F., Peyrin T. *Linear Cryptanalysis of the TSC Family of Stream Ciphers.* In: Roy B. (eds.) Advances in Cryptology - ASIACRYPT 2007. Lecture Notes in Computer Science, vol. 3788. Springer, Berlin, Heidelberg. 2005.

[3] Dinur, Itai; Shamir, Adi (2009-01-26). "Cube Attacks on Tweakable Black Box Polynomials" (PDF). Cryptology ePrint Archive. ePrint 20090126:174453.

[4] Dinur I., Shamir A. *Cube Attacks on Tweakable Black Box Polynomials.* Advances in Cryptology - EUROCRYPT 2009. Lecture Notes in Computer Science, vol. 5479. Springer, Berlin, Heidelberg. 2009.

[5] Pasalic, E.; *On Guess and Determine Cryptanalysis of LFSR-Based Stream Ciphers*; IEEE Transactions on Information Theory. Vol. 55 Ed.7º, 2009.

[6] Biryukov A., Shamir A. (2000) Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers. In: Okamoto T. (eds) Advances in Cryptology — ASIACRYPT 2000. ASIACRYPT 2000. Lecture Notes in Computer Science, vol 1976. Springer, Berlin, Heidelberg.

[7] Ding C.; *The differential cryptanalysis and design of natural stream ciphers*. In: Anderson R. (eds.) Fast Software Encryption. FSE 1993. Lecture Notes in Computer Science, vol. 809. Springer Berlin, Heidelberg.

[8] http://evc.cin.edu.ar/informacion consultada el 23/2/2018.